Post-quantum cryptography: the new era of cyber defence

How both the public and private sector can address the security threats that quantum computing could pose

July 2025

Authors

Juan Carlos Martín
SENIOR MANAGER

Elena Martín
SENIOR ASSOCIATE

Pietro Maria Rossi
ASSOCIATE

AXON CONSULTING

Contents

1. Revolutionising security: an introduction to post-quantum cryptography

Quantum computing – a type of computing that uses quantum mechanics to solve complex problems that are beyond the reach of classical computers – is still largely theoretical.

We explored this broader quantum context in our article *The Quantum Internet: For the good of all?*[1], which offers an introduction to the technologies shaping the quantum future.

Nevertheless, quantum computing is edging closer to practical reality, and when it reaches that point – potentially less than a decade from now – it could be applied to trusted modern encryption methods. The result? Quantum computers could crack codes in days that it might take a modern digital computer billions of years to beat.

It's no exaggeration therefore to say that cryptographic systems that secure our digital world face unprecedented risk.

Which is why, long before usable quantum computing actually exists, a system called post-quantum cryptography (PQC) is being discussed. PQC offers a proactive defence, leveraging new mathematical approaches that are resistant to both classical attacks and attacks using quantum computing.

Its benefits are, potentially, far-reaching, ensuring long-term data confidentiality, strengthens digital trust, and future-proofs sensitive infrastructure.

Many governments already accept this. Recognising the high stakes involved, governments around the world are accelerating PQC standardisation efforts, funding research into its use, and issuing guidance to prepare public and private sectors for the post-quantum era.

Long before usable quantum computing actually exists, a system called post-quantum cryptography (PQC) is being discussed. PQC offers a proactive defence, leveraging new mathematical approaches that are resistant to both classical attacks and attacks using quantum computing.

1 The Quantum Internet: For the good of all?

Of course, in reality, things aren't quite that straightforward. It's already clear that the transition to PQC won't be easy. How, for example, can we integrate a completely new technology within current systems without disrupting service delivery? And that isn't the only challenge associated with transitioning to a completely new approach to protecting information.

This paper aims to address these issues. Here we discuss the present-day state of both cryptography and PQC. the key benefits of PQC and also address the challenges adoption could bring.

In particular, we address the implementation process: how organisations can transition to quantum-resistant systems and frameworks to safeguard their digital ecosystems in a fast-approaching era of uncertainty brought about by the advent of quantum computing.

2. Traditional cryptography: the ancient art of hiding messages

What is cryptography, why does it matter, what threats does it face, and how can it be protected?

To answer this, we need to go back a couple of millennia to where the art of hiding information is thought to have begun: Ancient Greece. During the Peloponnesian War (431-404 BC), an ancient Greek war fought between Athens and Sparta for the leadership of the Greek world, the Spartans used a simple but effective way to send secret messages. They would inscribe a message on a piece of parchment that was coiled around a wooden stick known as a "scytale".

The message was meaningless after the parchment was unrolled because the letters were jumbled. The recipient would need an identical stick onto which the parchment could be rolled again to reveal the message.

Since those days, there have been numerous other examples of the uses of cryptography, from Julius Caesar's simple substitution cipher, in which a letter in what is known as plaintext is replaced by a letter some fixed number of positions down the alphabet ('and' becoming 'boe', say) to the much more complex World War II German Enigma machine and, more recently, blockchain-based systems.

Put very simply, cryptography is the practice of developing and adopting mechanisms (in modern times, coded algorithms) to protect and obscure data at rest and in transit. This ensures that such data may only be read by authorised people with the right 'keys' (pieces of information that secure communication and verify message authenticity) to process and decipher it.

Broadly speaking, we can summarise the essentials of cryptography in the following diagram:

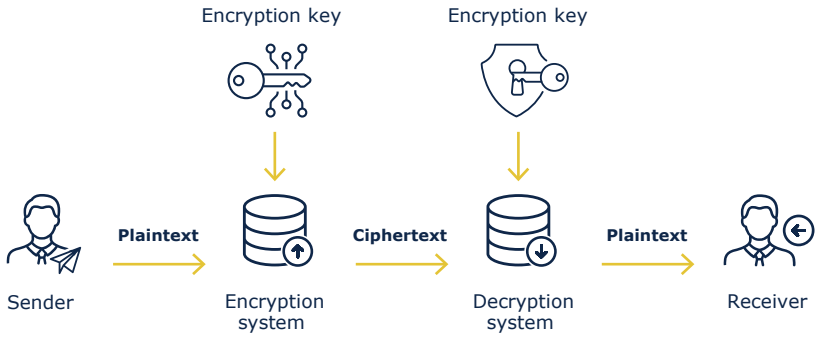

Figure 1: The essentials of cryptography

Figure 1 shows how cryptography is used to transform messages into a disguised format, known as ciphertext, that can only be rendered into a comprehensible format – or plaintext – by the authorised intended recipient through the use of a specific secret key. But it's not just about text, of course. Today cryptography can be used to encode any form of communication – audio, image, video or text.

Modern cryptography is based on four main principles, all of which guide the design and evaluation of secure systems: confidentiality, integrity, authentication and non-repudiation (see Figure 2).

CONFIDENTIALITY
Encrypted information can only be accessed by the person for whom it is intended using the secret key.

INTEGRITY
Encrypted information cannot be modified in storage or in transit without detecting alterations.

AUTHENTICATION
The identities of sender and receiver and the origin and destination of the information are confirmed.

NON-REPUDIATION
The sender cannot deny their intention to send the encrypted information once the transmission happened.

Figure 2: The four main principles of cryptography

Today's cryptographic techniques can be classified into three broad categories – depending on whether the encoding and decoding keys are public or private. These categories are symmetric cryptography, asymmetric cryptography and hybrid cryptography.

Symmetric cryptography

This is the most basic encoding method. Senders and receivers use the same key to encode and decipher data. While it by no means guarantees confidentiality, this method is at least fast and efficient.

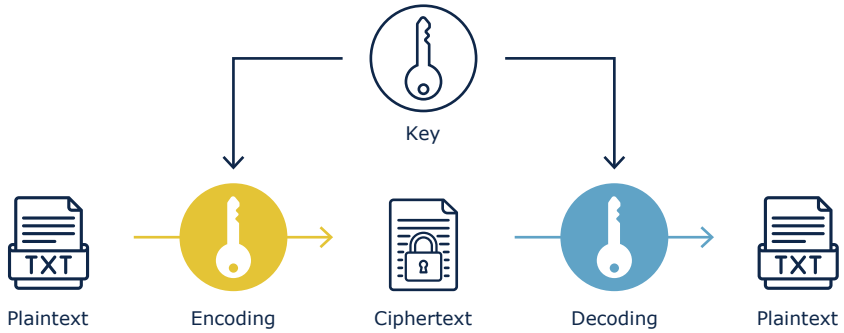

Figure 3: Symmetric encoding

Asymmetric cryptography

In this system, senders and receivers use different keys to encode and decode data. A public key, which can be freely shared, is used to encode plaintext, while a private key, available only to the receiver, is then used to decode ciphertext. Asymmetric encryption is a more reliable solution than the symmetric version, but is also more resource-intensive.

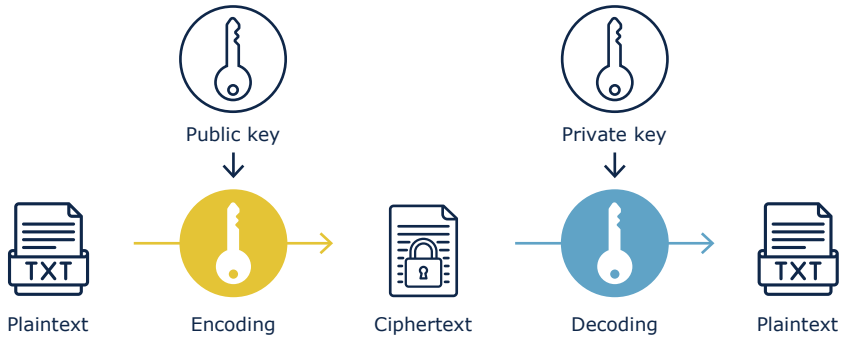

Figure 4: Asymmetric encoding

Hybrid cryptography

A hybrid solution combines elements of both of the earlier systems. A symmetric key is used to encode the message. The key itself is then encoded using a public key. The encoded symmetric key is transmitted together with the ciphertext. A private key is then used to decode the symmetric key, which will be used to decode the ciphertext and obtain the original message.

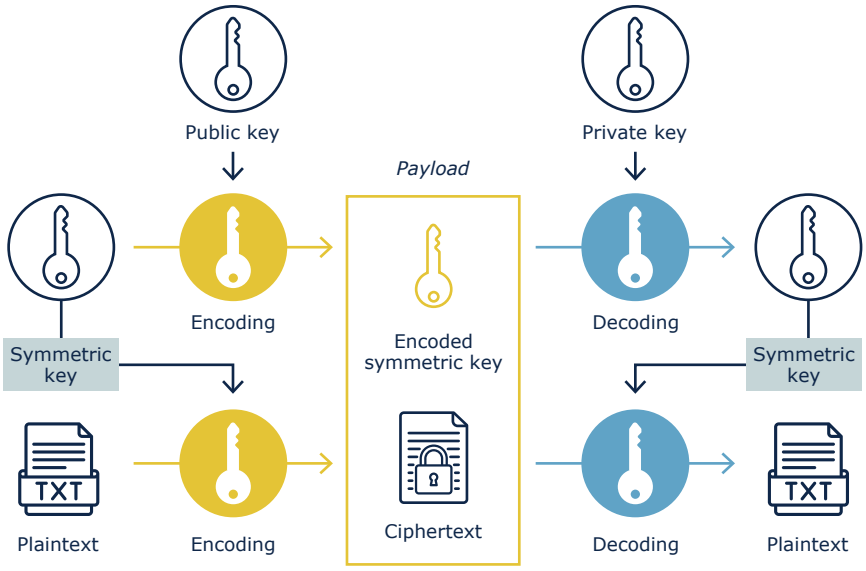

Figure 5: Hybrid encoding

Such conventional cryptography is used for securing digital communication today. At its most effective, its algorithms are virtually unbreakable by classical computers. Indeed, some encoding systems could require thousands or even millions of years to crack using current computational technology.

This perceived robustness has underpinned cryptography's strong role in data security. Today, Cryptography is used for everything from safeguarding financial transactions to protecting personal data. Today's cryptographic systems are often seen as the backbone of online security.

But how long can that last? As history has shown, no method of securing information is immune to human ingenuity. The Spartans' early encoding techniques were targeted by would-be code breakers. So too will be today's cryptographic systems. The drive to innovate and outsmart persists. Now, with quantum computing on the horizon, capable, in theory, of breaking in hours codes that would take classical computers millennia to decipher, the challenge is to keep cryptographic systems ahead of any potential threats.

A practical quantum computer is by no means a simple concept. It is a computer that makes use of the quantum states of subatomic particles to store information. What that means would take another paper to describe in detail. Suffice it to say that when the technology works, quantum computing will be able to carry out some tasks that are currently impossible on a traditional computer. It could also address tasks that could take billions of years for a modern computer – but complete them in weeks, days or even hours. One of these tasks is likely to be beating encryption: cracking our digital secrets.

We do not know precisely when this will happen – the first large-scale quantum computer is five – or more – years away. However, we do know one thing: the rise of quantum technologies exposes current cryptographic systems to significant risks, threatening critical infrastructures and data encoded using traditional cryptography. These technologies could undermine today's encryption methods, compromising the security of communications, financial transactions, and sensitive data.

The rise of quantum technologies exposes current cryptographic systems to significant risks, threatening critical infrastructures and data encoded using traditional cryptography.

Modern encryption typically relies on one public key-based encryption scheme in particular. It's called RSA (after its creators Rivest, Shamir and Adleman). The idea behind it is easy to multiply two large prime numbers together, but extremely difficult to reverse the process to factor the result.

In fact, a conventional computer could take billions of years for large enough numbers. By contrast, a quantum computer could factor large numbers exponentially quicker than traditional computers, making it possible to decipher any encrypted data in just a few days or hours. RSA isn't the only popular system that may not be able to outwit quantum computing. Another common scheme, elliptic curve cryptography (ECC) – based on the algebraic structure of elliptic curves over finite fields – is similarly vulnerable.

Of course most experts believe that large-scale quantum computers are not going to be developed for some years[2]. However, this will not prevent hostile or criminal groups from intercepting and storing encrypted data in the hope of decrypting it at a later date when advances enabled by quantum computing become available. This 'harvest now, decrypt later' strategy underlines the urgent need to adopt a new approach – and that is where post-quantum cryptography comes in.

2 Cryptographic Standards for a Post-Quantum World

3. Post-quantum cryptography: a whole new art of hiding messages

So, what is an appropriate response to these threats? Firstly, to counter the emerging risks posed by quantum computing, the global community must begin phasing out traditional cryptographic standards.

Why? Most importantly because a new class of cryptographic algorithms is needed – algorithms specifically designed to withstand the encryption-breaking capabilities of quantum computers. This is what post-quantum cryptography (PQC) can offer. Unlike conventional methods, PQC is built on algorithms that are believed to be resistant to both classical and quantum attacks, ensuring long-term data security in the face of advancing computational power.

Unlike conventional methods, PQC is built on algorithms that are believed to be resistant to both classical and quantum attacks, ensuring long-term data security in the face of advancing computational power.

These new algorithms are tailored to address two core cryptographic functions:

- General encryption, which secures data exchange across a public channel.
- Digital signatures, which verify identity and authenticity.

Unlike traditional encryption, which, as we have seen, often depends on factoring large numbers, PQC uses fundamentally different mathematical approaches. These approaches rely on different algorithms and techniques that experts believe will resist both classical and quantum attacks[3].

Examples of these techniques include systems that are lattice-based, code-based, hash-based, isogeny-based and multivariate.

3 Post-Quantum Cryptography – Current State and quantum mitigation

Lattice-based

In simple terms, this method hides information within a grid of points, making it hard to find without a special key.

A lattice is a regular arrangement of points in a multidimensional space – a 3D grid, like a cube made of dots, but extended into many dimensions. Lattice-based PQC encodes data as vectors, or arrows pointing to specific locations in this grid. It adds what is known as 'structured noise', slightly shifting these positions to obscure the message. Because the grid exists in many dimensions, the patterns can extend vastly through several points, making it almost impossible to decode the encrypted message among the endless options available – unless you know the correct key.

Code-based

Code-based cryptography disguises messages by adding errors in a way that only the intended recipient knows how to fix.

This method uses the theory of error-correcting codes (ECC). ECC techniques are used to detect and correct errors that occur during data transmission or storage. This type of cryptography takes a slightly different approach to ECC: it adds structured errors intentionally (that is, it adds extra bits to the original data). However, yet again, only the legitimate receiver can detect the errors with the code structure.

Hash-based

This approach uses special formulas to convert data into a fixed-length code that is almost impossible to reverse or fake.

Hashing is the process of transforming any given key or string of characters into another value. In this case, hash functions transform strings of arbitrary length into strings of fixed length called hash values – unique-looking codes that represent the original input in a compressed format. This ensures consistent output size regardless of input length (that is, regardless of whether the input is a message, a password or something else). Cryptographic hash-based functions are designed to be one-way; once the data is hashed, it is extremely difficult to figure out what the original input was just by looking at the hash value.

Isogeny-based

This method is built on complex relationships between mathematical curves and is extremely difficult to reverse-engineer.

Isogeny-based cryptography bases its approach on the challenge of finding the mathematical connection, called isogeny, between two elliptic curves – special types of curved graphs defined by equations – over finite fields – over finite fields. In practice, users start with a known curve and use a secret isogeny to reach another curve, which they share publicly. Even though these curves may look unrelated, the isogeny mathematically links them in a way that only the person with the secret can compute. The core concept is that it is easy to compute an isogeny, but it is extremely difficult, even for a quantum computer, to compute one between two given curves.

Multivariate systems

This last approach uses equations with many variables that are very hard to solve unless you know a hidden trick.

Multivariate cryptography is based on the difficulty of resolving systems of multivariate quadratic equations. Signature schemes can be built from these systems of equations. The signer uses a so-called 'trapdoor.' This is a secret transformation that turns the equations into something easy to solve. However, the resulting solution appears random to anyone that does not have the trapdoor.

These mathematical concepts – and others – have been used in recent years to build post-quantum encryption and signature scheme proposals.

Public agencies are already playing a vital role in these efforts, not only by shaping technical standards based on these concepts but also by driving adoption across both public and private sectors. Institutions like the US National Institute of Standards and Technology (NIST) have already laid the groundwork with resilient encryption standards, but continued government leadership will be essential to ensure secure and widespread implementation.

However, before looking more closely at the role of governments in the post-quantum era, let's remind ourselves of the benefits of PQC – and look at some of its challenges.

3.1.
Fortifying the future: the benefits of quantum-resistant solutions

As we have noted, the adoption of PQC is likely to bring with it some transformative benefits. Figure six highlights these benefits – and the next four sections examine them in more detail.

Figure 6: Expected benefits of post-quantum cryptography

3.1.1. Long-term data security

PQC provides robust protection for sensitive data, potentially ensuring its security for decades to come. We've already mentioned the possibility of criminals harvesting encrypted data now that could be unlocked at a future date. Transitioning to quantum-resistant algorithms is essential for safeguarding such data, protecting it against future quantum threats, maintaining long-term confidentiality and, as the next section reminds us, guaranteeing compliance with regulations.

3.1.2. Enhancing trust and compliance

As global data privacy laws impose increasingly stringent protection requirements, securing information against future quantum-based threats becomes a must. By adopting PQC, organisations can demonstrate a forward-thinking approach to security, ensuring they not only meet but exceed compliance standards. This proactive stance safeguards data against both current and emerging threats. Importantly too, it reinforces customer confidence.

3.1.3. Cost-effectiveness over time

Investing in PQC can also significantly reduce future costs associated with data breaches and regulatory fines – and offer substantial financial savings. Fines in particular can be significant. For example, following three major data breaches, the US Federal Trade Commission required hotel chain Marriott International, Inc. in 2024 to implement a robust information security program. Marriott also agreed to pay a $52 million penalty to 49 states and the District of Columbia.[4]

As for savings, according to a recent IBM report, organisations that adopt PQC can minimise the need for frequent and costly upgrades of encoding protocols, saving up to $2.2 million [5] every year.

3.1.4. Strengthening security infrastructure for organisations

The benefits of PQC extend beyond data protection. It can also strengthen an organisation's overall security framework. PQC can provide scalable security solutions, empowering organisations to expand and adapt as technological advances permit and requirements demand. In other words, it can help them in proactively safeguarding their infrastructure against future threats.

4 FTC Takes Action Against Marriott and Starwood Over Multiple Data Breaches

5 Cost of a Data Breach Report 2024

3.2. Challenges to PQC adoption

The process of standardising PQC algorithms and integrating them into existing infrastructure will complicate any transition. Three of the main issues facing a transition to PQC are:

- Implementation challenges
- Technological challenges
- Reputational challenges

These are addressed in the following three sections.

3.2.1. Implementation challenges

The transition to PQC brings with it a series of complex technical and operational challenges, many of which are discussed in more detail in a NIST NCCoE (National Cybersecurity Center of Excellence) 2021 white paper[6]. They include diverse algorithm needs, system and tooling overhaul, lack of cryptographic inventory and high migration costs.

Diverse algorithm needs
Different use cases will require distinct PQC algorithms. For instance, the size of a key or a signature may not be an issue in some applications but may be a problem in others. New applications must consider the requirements of PQC and give the new schemes (or, more accurately, new cryptographic protocols) time to adjust, reach maturity and be standardised.

System and tooling overhaul
Migration involves updating cryptographic libraries, hardware, operating systems, application codes, communications devices and protocols, not to mention user and administrative procedures.

Lack of cryptographic inventory
Before any transition to post-quantum algorithms takes place it is essential to identify where and for what purpose traditional cryptography is being used. After all, cryptography is widely integrated everywhere: in operating systems, applications, communications protocols, access control mechanisms and many operational technology (OT) systems. However, many organisations have not kept

6 Getting Ready for Post-Quantum Cryptography: Exploring Challenges Associated with Adopting and Using Post-Quantum Cryptographic Algorithms

track of its deployment; this will make it difficult to determine where post-quantum algorithms need to be implemented and what priority a specific algorithm needs to be given. Section 6.3 explains what this may involve.

High migration costs
The costs associated with migrating to PQC are expected to be substantial, primarily due to the complexity of identifying and accurately replacing existing public key algorithms with their post-quantum counterparts. In the US alone, the US Office of Management and Budget (OMB) estimates that the government-wide transition to PQC will cost $7.1 billion between 2025 and 2035w[7].

3.2.2. Technological challenges

Implementation challenges are not the only issues PQC brings with it. PQC also needs new types of communication networks; today's systems are not built to handle quantum-level security. New investments will be needed to find more affordable technology. One major challenge is going to be finding a way to send quantum data quickly and reliably over long distances. But new approaches, such as using particles or photons of light in ways that are difficult to tamper with unnoticed, could contribute to building faster, more secure communication systems.

3.2.3. Reputational challenges

Finally, there is public acceptance – a challenge that all new technology must eventually overcome. The prospect of broad adoption and use of quantum protocols is by no means totally trusted, especially by the public sector. Governments can manage this by guaranteeing prospective users and clients that data encoding will be safe on the computers hosting this new type of public key infrastructure.

Overcoming these barriers will require coordinated action and strong leadership. Governments and national agencies in particular have a key role to play in driving research, funding infrastructure upgrades and setting clear standards – a consideration that brings us to a discussion of that role.

7 OMB Report on post-quantum cryptography

4. Setting standards: the role of governments and national agencies

Many experts believe that as early as 2029 ongoing advances in quantum computing will make asymmetric cryptography vulnerable. By 2034 it could be fully breakable.[8] It is already becoming clear that a new mitigation strategy is required, and that conventional cryptographic techniques must be replaced.

National governments and international organisations are taking the first steps toward encouraging the development and adoption of practices that foster greater protection of systems.

Many experts believe that as early as 2029 ongoing advances in quantum computing will make asymmetric cryptography vulnerable. By 2034 it could be fully breakable. It is already becoming clear that a new mitigation strategy is required, and that conventional cryptographic techniques must be replaced.

PQC in the USA

The USA was among the first countries to initiate a structured transition towards PQC. Indeed, it published the first government-approved cryptographic tools.

As early as November 2022, the Office of the President of the United States issued a memorandum called Promoting United States Leadership in Quantum Computing while Mitigating Risk to Vulnerable Cryptographic Systems[9]. The memorandum described preparatory steps to be undertaken by agencies to begin their transition to PQC by conducting a prioritised inventory of critical and sensitive systems.

This continued in August 2024, when the first PQC standards arrived via NIST. After more than eight years of joint work between government, academia, and industry, three new Federal Information Processing Standards (FIPS), as they are called, were issued. These standards are regarded as the first formally approved PQC algorithms. They are an early strategic and technical milestone for PQC adoption across federal agencies and critical infrastructure systems.

8 Begin Transitioning to Post-Quantum Cryptography Now

9 Memorandum for the Heads of Executive Departments and Agencies

Next, in January 2025, President Biden issued Executive Order 14144 which, among other aspects, required the Cybersecurity and Infrastructure Security Agency (CISA) to compile and maintain a catalogue of PQC-enabled products which, it is hoped, will be a centralised reference to support federal agencies in adopting PGC solutions. In June 2025, President Trump amended the Order, easing certain mandates but maintaining CISA's responsibility over the PQC product catalogue.

PQC and the EU

The European Union has also advanced efforts to coordinate a secure and harmonised approach to PQC adoption.

An early example of this happened in April 2024, when the European Commission (EC) published its *Recommendation on a Coordinated Implementation Roadmap for transition to Post-Quantum Cryptography*[10] to encourage Member States to develop and implement a harmonised approach as the EU transitions to PQC.

Reinforcing this commitment, in December 2024, 18 Member States, issued a statement[11] supporting the EC-led effort to encourage PQC migration and emphasising the need for public and private entities to "make the transition to post-quantum cryptography a top priority". The statement urges these entities to initiate the transition by conducting a quantum threat analysis and creating a risk-based migration roadmap.

About six months later, in June 2025, Member States, in collaboration with the Commission, issued a timeline and roadmap for the transition to PQC.[12] This document divides the recommended approach into two parts – First Steps and Next Steps – emphasising informed stakeholder engagement and cryptographic asset management. It also proposes a transition timeline, one that sees national PQC strategies initiated by 2026, the transition of high-risk systems to PQC by 2030, and widespread adoption of PQC by 2035.

Public entities and other critical infrastructure sectors, particularly those covered by the NIS2 Directive, a European Union law focused on enhancing cybersecurity across the EU, fall within the scope of the timeline and are advised to use it as a reference.

10 Recommendation on a Coordinated Implementation Roadmap for the transition to Post-Quantum Cryptography

11 Securing Tomorrow, Today, Transitioning to Post-Quantum Cryptography

12 A Coordinated Implementation Roadmap for the Transition to Post-Quantum Cryptography

Other regions – and the private sector

As we have seen, the adoption of PQC is no longer just a theoretical concern. It is a concrete priority. Both policy infrastructure and financial resources are being committed to quantum strategies. Countries worldwide are investing in research and development in what could be called a quantum race. PQC will be a part of this.

The UK, for example, has planned an investment of £2.5 billion over the next ten years as part of its National Quantum Strategy. By 2033, the UK expects that 75% of relevant business will have taken steps towards adopting quantum computing[13]. This will, or should, go hand in hand with a security strategy embracing PQC.

However, the public sector is not alone in embracing PQC. Private organisations have launched initiatives to ensure cryptographic resilience. For instance, Microsoft has established the Microsoft Quantum Safe Program (QSP) with the goal of achieving quantum readiness by integrating PQC algorithms across Microsoft's products and services.[14]

13 National Quantum Strategy

14 Microsoft's quantum-resistant cryptography is here

5.
Leading the way: NIST's first PQC algorithms

We have already briefly mentioned that standards are now part of the PQC story. In August 2024, NIST released the first three Post-Quantum Encryption Standards (see tables below). These can help to support responses to potential attacks from a quantum computer and, more generally, to secure any form of electronic information and communication.

These standards are designed to cover essential encryption tasks: that is, general encryption and digital signatures. They contain encryption algorithms, the instruction to implement them and how they are used. Indeed, NIST is already encouraging entities to use them, saying: "We encourage system administrators to start integrating them into their systems immediately because full integration will take time."[15]

In August 2024, NIST released the first three Post-Quantum Encryption Standards (see tables below). These can help to support responses to potential attacks from a quantum computer and, more generally, to secure any form of electronic information and communication.

Code: FIPS 203[16]

Name: Module-Lattice-Based Key-Encapsulation Mechanism Standard

Description: FIPS 203 defines a key-encapsulation mechanism (KEM) based on lattice cryptography used by two parties to establish a shared secret key over a public channel. This ensures that, under certain conditions, both parties will produce the same key and keep it secret from potential attackers. These quantum-resistant keys can then be safely used by symmetric algorithms to encrypt or authenticate digital information conforming to a hybrid cryptographic system.

Code: FIPS 204[17]

Name: Module-Lattice-Based Digital Signature Standard

Descripton: FIPS 204 specifies the CRYSTALS-Dilithium algorithm, a lattice-based signature scheme for applications that require a digital (rather than handwritten) signature. It detects unauthorised

15 NIST Releases First 3 Finalized Post-Quantum Encryption Standards
16 FIPS 203 – Module-Lattice-Based Key-Encapsulation Mechanism Standard
17 FIPS 204 - Module-Lattice-Based Digital Signature Standard

modifications of stored or transmitted data and authenticates the signatory's identity. The algorithm uses a pair of keys: a private key for signature generation uses and a public key for verifying a signature. Only the private key holder can generate a verifiable signature, which is provided with the signed data and verified using the signatory's public key.

Code: FIPS 205[18]

Name: Stateless Hash-Based Digital Signature Standard

Description: FIPS 205 is also for applications requiring a digital signature instead of a written signature. It works similarly to FIPS 204 but is hash-based cryptography (called a SPHINCS+ algorithm), providing an alternative to FIPS 204 with strong security guarantees but larger signature sizes and slower speeds.[19]

These standards are more than just technical specifications; they are the first government-endorsed cryptographic tools, designed to survive in the quantum era. Public agencies are expected to begin adapting their cryptographic systems to align with these standards. At the same time, the private sector is being encouraged to build secure systems and modernise software supply chains.

However, this is not a one-time effort. NIST has already started evaluating additional algorithms and backup plans in case of potential attacks that defeat those algorithms. Other standards are on the way.

A fourth standard, FIPS 206, is expected to standardise the FALCON algorithm, a lattice-based digital signature scheme which targets strong security combined with efficient performance. This is particularly useful for services requiring fast verification times. FIPS 206 was anticipated for official release in late 2024. A draft release is now expected in late 2025 for public comments.

A fifth algorithm – a Hamming Quasi-Cyclic (HQC) (code-based) algorithm – has been selected as an alternative or secondary standard to FIPS 203. FIPS 207 is expected to be finalised and released before 2027.[20]

18 FIPS 205 – Stateless Hash-Based Digital Signature Standard

19 Performance and Applicability of Post-Quantum Digital Signature Algorithms in Resource-Constrained Environments

20 NIST Selects HQC as Fifth Algorithm for Post-Quantum Encryption

6. Deploying PQC: the first steps

As we have noted throughout this paper, implementing PQC is a critical step for organisations aiming to secure their data against emerging quantum threats. But what does this mean in practice?

Put simply, this process involves establishing a department responsible for coordinating the transition, assessing current cryptographic systems, identifying vulnerabilities, and transitioning to quantum-resistant algorithms that ensure long-term security.

While such a shift requires careful planning and coordination, it also presents an opportunity to modernise existing infrastructures and align them with future security standards. By adopting a structured approach to implementation, organisations can mitigate potential risks, maintain compliance with evolving regulations, and establish a resilient foundation on which to build the safeguarding of sensitive information in the quantum era.

The following steps (summarised in Figure 7) should be taken by public or private organisations adopting PQC.

By adopting a structured approach to implementation, organisations can mitigate potential risks, maintain compliance with evolving regulations, and establish a resilient foundation to safeguard sensitive information in the quantum era.

- **CRYPTO CENTRE OF EXCELLENCE:** Establish a CCoE to assess the scope, impact and cost of the transition and coordinate cryptographic policy and teams providing expertise for the transition.
- **QUANTUM-READINESS ROADMAP:** Develop a quantum-readiness roadmap to define objectives to reach, including timelines, resource allocation and any necessary changes to infrastructure and systems.
- **CRYPTOGRAPHIC INVENTORY:** Conduct an inventory of the cryptography algorithms in use in the organisation, identifying all applications and communication channels used to secure sensitive data.
- **VENDOR COLLABORATION:** Connect with vendors to understand their plans to move to post-quantum cryptography, the implementation roadmap and the potential impact of upgrades to existing systems.
- **ALGORITHMS DEPLOYMENT:** Implement PQC algorithms and protocols across systems and applications coordinating the transition without compromising security or functionality.
- **PERFORMANCE MONITORING:** Monitor the performance and security of the systems conducting regular assessments and updates to address new threats and maintaining compliance with industry standards.

Figure 7: Post-quantum cryptography implementation process

6.1. Create a crypto centre of excellence

Establishing a dedicated department to manage the transition to PQC is the first step toward ensuring a coordinated shift to quantum-resistant systems.

Such a department (or departments) should employ experts in cryptography, cybersecurity, IT, software engineering, compliance, risk, and project management. This diverse expertise will ensure that the transition addresses all potential organisational impacts, such as regulatory compliance or internal training.

The responsibilities of the department will include assessing the current landscape, identifying systems vulnerable to quantum threats, prioritising areas for transition, developing a roadmap and coordinating with stakeholders for the integration of quantum-resistant algorithms.

6.2. Establish a quantum-readiness roadmap

This step involves a comprehensive evaluation of current encoding methods to identify vulnerabilities that could be exploited by quantum algorithms. Key components of this roadmap (addressed in more detail below) will include the activities to be executed, establishing timelines for the migration process and defining KPIs and monitoring mechanisms. Additionally, such a program must emphasise ongoing education and training to ensure that employees at all levels understand the implications of quantum threats and their own role in maintaining a secure environment.

6.3. Prepare a cryptographic inventory

Preparing cryptographic inventories can provide a clear understanding of an organisation's current situation. This process involves cataloguing all systems, applications, and protocols that rely on cryptographic methods and secure communications. It should thereby be possible to obtain a holistic view of where vulnerabilities might exist as quantum computing evolves. The inventory should also evaluate the criticality of each system and its exposure to external threats, enabling organisations to prioritise systems for migration based on risk assessments.

6.4. Collaborate with technology vendors

Most critical systems and applications rely on third-party technologies. Organisations must engage with vendors early in the transition process to make sure that their products and services are compatible with quantum-resistant algorithms. Key considerations will include validating whether vendors are adopting quantum-safe standards, their timelines for updates, and their ability to support the migration of existing systems without disruptions.

6.5. Implement post-quantum cryptography algorithms

This simply means integrating quantum-resistant algorithms into existing systems, ensuring they replace or complement current cryptographic methods without compromising functionality. Deployment should begin with systems identified as most critical or vulnerable during the cryptographic inventory and risk assessment phases. Deployment processes should be designed to avoid (or minimise) service disruption.

Of course pilot testing is essential. This will help to validate the performance, interoperability, and reliability of the new algorithms in real-world scenarios before organisation-wide implementation.

6.6. Assess the organisation's operations

It will also be essential to thoroughly evaluate the performance of quantum-resistant algorithms, including their impact on system performance, interoperability, and data protection. Key metrics such as encoding speed, compatibility with legacy systems, and the reliability of secure communications should be closely monitored through regular audits, penetration testing and user feedback.

7. Conclusion: It’s time for a quantum leap. Are you ready?

Cybersecurity is under threat – not now, but relatively soon. Post-quantum cryptography is a solution that anticipates a future in five to ten years when current encoding methods could be unable to combat the computational power of quantum computers, making data easily accessible by outsiders.

Does this still seem like a manageable timescale? Perhaps, but right now malicious actors are storing encrypted data, expecting to decrypt it when quantum computers allow. Which is why organisations should start the process of transitioning to PQC immediately.

In any case, transitioning to PQC will bring substantial long-term benefits: enhanced data protection, improved compliance and reputation, future cost savings, and a stronger, more resilient security infrastructure.

That is not to say this will be easy. This process presents significant challenges, including high implementation costs, infrastructure upgrades, and the need to build user trust in new security systems.

The good news is that, to overcome these challenges, governments and international agencies are already boosting research into, and development of, quantum computing and its security implications, financing major investments and establishing technological leadership.

Regulatory and national bodies are also playing a part. NIST in the US has recently released the first three post-quantum encoding standards. FIPS 203, which corresponds to a set of algorithms for establishing a shared secret key over a public channel for encoding and decoding, and FIPS 204 and FIPS 205, which are sets of algorithms used as digital signatures to detect unauthorised modifications of data and to authenticate the identity of the signatory. More standards will follow.

What, then, is the key takeaway of this paper? The transition to PQC is a major challenge – but it is unavoidable. Governments and companies need to start the transition as soon as possible. To implement post-quantum encoding, all organisations should already be addressing potential challenges. Delay could, at the least, risk inviting serious cyberthreats. At the worst it could mean the collapse of critical infrastructure, with consequences affecting every part of society.

About
Axon Partners Group

Axon Partners Group is an international firm founded in 2006 that provides investment and advisory services to a broad client base in the ICT and digital space in more than 70 countries across the world.

Axon's emerging technologies practice is at the core of our work and a growing priority for clients. We focus on strategy, policy, and market intelligence around a broad spectrum of next-generation technologies, engaging both private and governmental stakeholders. By partnering closely with decision-makers, Axon helps them anticipate trends, address critical challenges, and develop actionable roadmaps to harness the full potential of emerging technologies.

Tel: +34 913 102 894
Email: marketing@axonpartnersgroup.com